ITUpcycle LLC Privacy and Data Security Policy

Updated September 2025

1. Executive Summary: The Foundation of Trust and Compliance

1.1. Statement of Purpose

This document presents a comprehensive, expert-level IT Asset Disposition (ITAD) Privacy and Data Security Policy for the company ITUpcycle LLC. The policy is designed to serve as a foundational element of the company's operations, ensuring that all client data, both operational and residing on retired IT assets, is handled with the utmost security, integrity, and regulatory compliance. This framework positions ITUpcycle LLC as a trusted partner committed to the dual objectives of data protection and sustainable asset value recovery.

1.2. Core Policy Commitments

The policy is structured around three fundamental principles. The first is an unwavering commitment to absolute data security, assuring that all client information is rendered unrecoverable from assets entrusted to the company. The second is a dedication to multi-jurisdictional regulatory compliance, with processes engineered to meet and exceed stringent global and national standards such as GDPR, CCPA/CPRA, and HIPAA. The third is the principle of complete transparency, accomplished through a meticulously documented chain of custody and verifiable proof of destruction.

1.3. A Dual-Focus Approach

ITUpcycle LLC's business model is predicated on maximizing asset value through upcycling, recycling, and remarketing, which distinguishes it from traditional ITAD providers. This policy demonstrates that this focus on value recovery is not in conflict with our commitment to data security. On the contrary, it is a seamless extension of the company's dedication to certified, secure, and environmentally responsible asset management, leveraging methods like cryptographic erasure that protect data while preserving asset value.

2. Introduction to ITUpcycle LLC's Privacy and ITAD Policy

2.1. Policy Scope and Applicability

This policy applies to all data and IT assets processed by ITUpcycle LLC, irrespective of their origin, type, or final disposition. Its governance extends to the limited business information collected from clients for service delivery and, crucially, to the sensitive data contained within the IT assets themselves. A modern ITAD policy must not be narrowly focused on traditional assets like computers and servers. The analysis of client needs reveals that data can be found on a vast array of devices, including printers, networking equipment, medical devices, and IoT hardware. A failure to address these non-traditional assets creates a significant, often overlooked, security liability for both the client and the ITAD provider. This policy therefore establishes a universal and consistent process for all data-bearing devices to ensure no risk is left unaddressed.

2.2. Guiding Principles

The operational philosophy of ITUpcycle LLC is guided by a set of core principles that underpin this policy.

- **Data Security as a Prerequisite:** The foremost objective of any ITAD process is to render all client data completely unrecoverable, regardless of whether the asset is destined for remarketing or physical destruction.
- **Transparency and Accountability:** Every stage of the ITAD process, from the initial collection to the final disposition, is meticulously documented. This meticulous record-keeping provides a full audit trail and a legally defensible chain of custody, which is vital for demonstrating compliance and accountability to clients and regulators.
- **Compliance by Design:** All of the company's processes are engineered to meet and exceed global, national, and industry-specific privacy and security standards from the very beginning. This includes adherence to frameworks such as GDPR, CCPA, and HIPAA, ensuring that compliance is an inherent part of the service, not an afterthought.
- **Data Minimization:** ITUpcycle LLC is committed to collecting, using, and retaining only the bare minimum of client-provided business information necessary to effectively provide its services and maintain compliant records.

2.3. Key Definitions

- **IT Assets:** This is a broad term that encompasses any hardware device that may contain data. This includes, but is not limited to, servers, laptops, desktops, mobile phones, tablets, printers, networking equipment, medical devices, point-of-sale (POS) systems, and other general e-waste items with a cord or battery.
- **Client Data:** This refers to all information, including confidential, proprietary, and personally identifiable information (PII), that resides on the IT Assets entrusted to ITUpcycle LLC.
- **Personally Identifiable Information (PII):** As defined by various global privacy frameworks like GDPR and CCPA, PII includes data that can be used to identify an individual. This can range from basic contact information like a name and email address to more sensitive details like financial account numbers, social security numbers, and health information.
- **Chain of Custody:** This is the chronological, documented history of an IT asset's movement, handling, and disposition from the moment it is collected to its final state.

3. Data Handling and Processing: Website and Business Operations

3.1. Information We Collect (Our Operational Data)

Upon commencement of providing services, ITUpcycle LLC collects limited business-related information from its clients. This information is a necessary component of service delivery, allowing for communication, order processing, and documentation. The data collected directly from clients may include their name, job title, company name, address, email address, and phone number, all essential for fulfilling service requests. Additionally, transactional data such as payment information is collected to process service fees.

The company's website also collects certain information indirectly through the use of tracking technologies. As is standard for most websites, ITUpcycle LLC uses cookies and similar technologies, such as web beacons and tags, to track activity and gather analytical data. This information includes internet protocol (IP) addresses, browser type, and user interaction patterns. It is important to note that this data is primarily used to analyze trends, improve website functionality, and personalize the user's experience by remembering preferences. The company explicitly states that it does not use these technologies to track individuals across the web or for targeted advertising, nor does it associate browsing behavior with a personal identity.

2. How We Use Your Information

The business-related information collected by ITUpcycle LLC is used exclusively for legitimate business purposes.

- **Service Fulfillment:** The primary use of this information is to process service orders, generate legally defensible Certificates of Destruction, and provide detailed, serialized asset reports to clients.

- **Communication:** Client contact information is used to respond to inquiries, provide updates on service status, and send essential transactional messages, such as order confirmations or completion notifications.
- **Service and Website Improvement:** Aggregated data and client feedback are used to continually improve the company's services and enhance the functionality of its website.
- **Legal and Compliance Obligations:** Information such as asset reports and Certificates of Destruction is retained to maintain audit-ready records and to comply with legal obligations, including responding to legal inquiries or regulatory audit requests.

3.3. Information We Do Not Collect (From IT Assets)

A critical component of this policy, and a key factor in building client trust, is the explicit and unwavering commitment to not collecting or accessing any data residing on the client's IT assets. This distinction is crucial and positions ITUpcycle LLC as a secure data guardian, rather than a potential data risk. Unlike many technology companies that monetize data, ITUpcycle LLC makes a clear statement that it does not access, copy, reproduce, or retain any client data from the IT assets it processes.

This commitment extends to all forms of client information, including personal files, emails, configuration data, device usage logs, and software keys or credentials. By taking this proactive stance, the company establishes a professional boundary with its clients' core business data, which is essential for ensuring security and mitigating liability. This approach reassures clients that their data is not viewed as a potential revenue stream through data analysis or brokering but is handled with the singular purpose of secure and irreversible destruction or sanitization.

4. Secure IT Asset Disposition: A Focus on Outcomes

4.1. The ITAD Lifecycle and Guaranteed Data Destruction

The ITAD process at ITUpcycle LLC is not a simple, linear path but a dynamic decision-making process based on the asset's condition, its potential for value recovery, and the client's specific instructions. The process begins with secure logistics and the establishment of a robust chain

of custody. Upon pickup, every IT asset is immediately scanned, serialized, and documented. This action creates a real-time digital record that tracks the asset's movement from the moment of collection to its final disposition, providing a complete audit trail and unparalleled customer transparency.

The company guarantees that all data-bearing devices, regardless of their final outcome, will be subjected to certified data destruction methods that render all data completely and irreversibly unrecoverable. This commitment is central to the company's value proposition and a fundamental requirement for meeting industry-leading standards.

4.2. Certified Data Destruction Methods

ITUpcycle LLC employs a range of data destruction methods, with the specific choice determined by factors such as data sensitivity, the asset's residual value, and compliance requirements. All methods are executed in strict accordance with recognized industry standards.

- **Physical Destruction:** This is the most definitive method for data destruction. It involves the physical obliteration of the storage medium through shredding, pulverization, or degaussing for magnetic media.[3] This method is the preferred choice for assets with no residual value or for highly sensitive information, such as classified government or proprietary company data, where the absolute certainty of non-recoverability is paramount.
- **Cryptographic Erasure:** For encrypted devices that have remarketing potential, this method is a core competency for ITUpcycle LLC. It involves destroying the encryption keys used to access the data, which renders the data irretrievable while preserving the asset's physical integrity for future reuse or resale. This approach is highly efficient and aligns perfectly with the company's mission to maximize asset value.
- **Software Wiping/Overwriting:** For non-encrypted media with reuse potential, the company performs multiple overwrites of all data storage areas. This process adheres to the "Clear" and "Purge" methods defined in NIST 800-88 Revision 1 guidelines.

4.3. Transparency through Documentation

To provide clients with auditable proof of service, ITUpcycle LLC provides comprehensive documentation at every stage of the process.

- **Certificate of Destruction (CoD):** This is a legally defensible document provided for every data-bearing asset. It includes the asset's unique serial number, the specific data destruction method used, and the date and time of destruction. The CoD serves as essential proof of compliance for audits and legal defense.

- **Asset Reports:** The company provides comprehensive reports that detail the inventory, condition, and final disposition of each asset, further enhancing transparency.

Table 1: IT Asset Types and Potential Data Contamination Risks

IT Asset Category	Example Devices	Potential Data Contamination Risks
End-User Compute	Desktops, Laptops, Thin Clients, Monitors	PII, proprietary business data, financial records, passwords, email data
Data Center	Servers, Storage Arrays, Networking Hardware (Routers, Switches)	PII, confidential client data, financial information, intellectual property, infrastructure credentials
Mobility & IoT	Phones, Tablets, Handheld Devices, Smart Watches	PII, precise geolocation data, health information (if fitness tracking), financial data
Specialized Equipment	Medical Devices, POS Systems, Multifunction Devices (MFD)	PII (scanned documents), Protected Health Information (PHI), payment card data, transactional records, network credentials

Table 2: Data Destruction Methods and ITAD Outcomes

IT Asset Type	Data Sensitivity Level	Recommended Destruction Method	Applicable Standard	Final Disposition Outcome
Laptops, Servers	Low-Medium (non-sensitive PII)	Software Wiping/Overwriting	NIST 800-88 Clear/Purge	Resale, Redeployment, Donation
Laptops (encrypted)	Medium-High (proprietary data, PII)	Cryptographic Erasure	NIST 800-88 Clear	Resale, Redeployment, Donation
Hard Drives, SSDs	High (PHI, financial, classified)	Physical Shredding or Pulverization	NIST 800-88 Destroy, NAID AAA	Material Recycling
Magnetic Media	All levels	Degaussing	NIST 800-88 Purge	Material Recycling
Printers, POS Systems	Medium-High (cached data)	Physical Shredding of media	NIST 800-88 Destroy	Material Recycling

5. Legal and Regulatory Compliance

5.1. ITUpcycle LLC's Role as a Service Provider

ITUpcycle LLC operates as a data processor on behalf of its clients, who are the data controllers. In this role, the company is committed to processing data only as instructed by the client and in strict accordance with this policy and all applicable laws. The company is not a data broker and does not sell or share any client data with third parties for marketing or advertising purposes.

5.2. Compliance with Global Data Protection Frameworks

The company’s processes are engineered to satisfy the requirements of major international privacy regulations.

- **General Data Protection Regulation (GDPR) and UK GDPR:** As a data processor, ITUpcycle LLC's procedures are built around the core principles of GDPR. The company's policy is written in clear, intelligible language and is easily accessible, ensuring transparency. The company retains client business data under the legal basis of contract fulfillment and legitimate interest, and it provides mechanisms for data subjects to exercise their rights to access, rectification, erasure, and data portability.
- **California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):** The company adheres to the rights conferred upon California consumers, including the Right to Know, Right to Delete, Right to Opt-Out, Right to Correct, and Right to Limit the use of sensitive information. In its capacity as a service provider, ITUpcycle LLC recognizes that it is not directly responsible for responding to consumer requests directed to its clients, but it will fully cooperate with clients to facilitate the fulfillment of these requests. The company's business model is inherently compliant with the CCPA's non-sale provisions, as it does not sell or share personal information.
- **Health Insurance Portability and Accountability Act (HIPAA):** The company understands that if a client is a Covered Entity and entrusts it with Protected Health Information (PHI), ITUpcycle LLC becomes a Business Associate. In such cases, the company will execute a Business Associate Agreement (BAA) that outlines the permissible uses and disclosures of PHI and commits the company to implementing all necessary safeguards. This legal and operational obligation extends to all of the company's own

downstream partners, creating a chain of HIPAA compliance that protects the entire data lifecycle. Failure to extend this contractual obligation to subcontractors exposes the entire chain to liability, underscoring the necessity of this sophisticated approach.

5.3. Compliance with Other Key US Regulations

The company’s comprehensive approach to data security extends to other key US regulations.

- **Gramm-Leach-Bliley Act (GLBA):** The company's secure disposition methods are designed to protect the non-public personal financial information of consumers, as required by GLBA.
- **Fair and Accurate Credit Transactions Act (FACTA):** The company ensures that consumer credit information is securely and irreversibly destroyed to prevent unauthorized access and comply with FACTA's Disposal Rule.
- **Payment Card Industry Data Security Standard (PCI DSS):** The company's processes for handling assets with cardholder data meet the strict disposal requirements of PCI DSS.
- **Family Educational Rights and Privacy Act (FERPA):** The company is equipped to handle and destroy educational records in compliance with FERPA.
- **State Data Destruction Laws:** Recognizing the lack of a single comprehensive federal law, the company’s policy is to comply with the "reasonable measures" standards required by the various state laws that mandate the destruction of personal information.

5.4. Adherence to Industry Standards and Certifications

ITUpcycle LLC's commitment to security and compliance is validated by adherence to leading industry standards. The company’s processes are aligned with NIST 800-88 Revision 1 guidelines for data sanitization and destruction. The company seeks to obtain or work with partners who hold certifications such as R2v3 (Responsible Recycling) for environmental stewardship and NAID AAA (National Association for Information Destruction) for secure data destruction, demonstrating a verified commitment to the highest level of security and accountability.

Table 3: Regulatory Compliance and ITAD Policy Requirements

Regulation	Covered Data Type	Key ITAD Policy Requirement	Corresponding Policy Section
HIPAA	Protected Health Information (PHI)	Formal Business Associate Agreement (BAA), auditable safeguards, secure destruction of PHI	5.2 (HIPAA), 6.1 (Third-Party Management), 7.2 (Technical Safeguards)
CCPA/CPRA	Personally Identifiable Information (PII)	Service Provider status, cooperation on Right to Delete requests, non-sale of data	5.2 (CCPA), 3.3 (Data We Don't Collect), 6.1 (Third-Party Management)
GDPR	Personal Data	Transparent policy, data subject rights (e.g., erasure), secure processing, cross-border transfer safeguards	5.2 (GDPR), 8.2 (Your Rights)
GLBA	Non-Public Personal Financial Info	Secure and documented destruction of financial data on all media	4.2 (Data Destruction Methods), 5.3 (Other US Regulations)
FACTA	Consumer Credit Information	Secure disposal and certified destruction of consumer reports	4.2 (Data Destruction Methods), 5.3 (Other US Regulations)

6. Third-Party Management and Data Sharing

6.1. Limited Disclosure and Service Providers

ITUpcycle LLC's operational model, which includes a focus on asset value recovery and recycling, necessitates the use of a network of certified downstream partners and logistics providers. The company's policy explicitly addresses this by stating that it will not sell, lease, or share client business or company data with third-party marketers, advertisers, or data brokers. This is a crucial point of differentiation and trust-building.

Information is shared only on an as-needed basis with certified logistics and downstream partners, and only under a strict contractual obligation. This contractual agreement ensures that these partners are bound to meet the same stringent data protection and security standards outlined in this policy, thereby mitigating the inherent risk associated with entrusting data to external entities. The need for specialized services from downstream providers creates an operational requirement for data sharing; however, this is a controlled and monitored process designed to extend the company's commitment to security across the entire ITAD chain.

6.2. Due Diligence and Oversight

Before engaging any downstream partner, ITUpcycle LLC conducts thorough due diligence to ensure their competency, integrity, and compliance. This process includes a review of their certifications, such as R2 and NAID AAA, and a requirement for a written agreement that includes explicit data destruction and confidentiality clauses. This due diligence and ongoing oversight provide assurance that the client's data is protected even when handled by third parties, a critical component of a truly secure ITAD solution.

7. Data Security Safeguards: A Multi-Layered Approach

ITUpcycle LLC employs a robust, multi-layered security framework that incorporates physical, technical, and administrative safeguards to protect all data it handles. This comprehensive approach is designed to prevent unauthorized access, use, or disclosure of information.

7.1. Physical Safeguards

Physical security measures are the first line of defense against unauthorized access. The company's facilities are protected by a comprehensive system that includes electronically secured perimeter doors, 24/7 video surveillance, audited entry-point records, and secure, access-controlled entry points. Internally, IT assets are stored in a segregated, climate-controlled, and access-controlled area from the moment they are received until their final disposition.

7.2. Technical Safeguards

To protect limited client business information retained for service records, the company implements a range of technical safeguards. These include the use of encrypted file storage and secure communications channels. All internal systems are protected by firewalls and are subject to continuous monitoring to detect and prevent malicious or fraudulent activity. Access to data is controlled through a role-based access system, ensuring that employees can only access the minimum amount of information required for their specific job function.

7.3. Administrative Safeguards

Administrative controls are a key component of the company's security posture. All employees undergo mandatory data security and privacy training, which covers the principles outlined in

this policy and the legal obligations it addresses. Furthermore, ITUpcycle LLC maintains a detailed and regularly tested incident response plan for security incidents and data breaches. This plan includes clear protocols for a swift and effective response, including notification procedures for affected clients and relevant authorities, ensuring accountability and transparency in the event of a security event.

8. Data Retention, Client Rights, and Policy Governance

8.1. Data Retention Policy

ITUpcycle LLC's data retention policy is guided by the principle of data minimization. The company retains only the limited client business information necessary to fulfill service requests, comply with legal and regulatory obligations, and for audit purposes. This includes records such as asset reports and Certificates of Destruction. Critically, the company does not retain any client data from the IT assets themselves.

Retention periods are defined by legal requirements (e.g., for tax, accounting, and reporting purposes) and are subject to periodic review to ensure that no data is retained for longer than is necessary. Once a retention period has expired, the information is securely disposed of by removing all files and backups from company systems.

8.2. Your Rights and Choices

Clients of ITUpcycle LLC retain certain rights regarding the limited business information the company has collected. Clients have the right to request a copy of this information, to request its deletion, or to correct any inaccuracies. The company will fulfill these requests within a reasonable timeframe, subject to its legal and audit obligations.

8.3. Policy Review and Updates

The IT and regulatory landscapes are in a constant state of flux. To ensure ongoing compliance with new regulations and evolving industry best practices, this policy will be reviewed and updated at least annually, or as needed, to reflect any changes in legal requirements or operational procedures. Any changes will be posted on the company's website, and continued use of services will constitute acceptance of the updated policy.

9. Appendices

Appendix A: Glossary of Legal and Technical Terms

- **Business Associate:** A person or entity, other than a member of a covered entity's workforce, who performs functions or activities on behalf of a covered entity that involve access to protected health information.
- **Chain of Custody:** The chronological history of an IT asset's movement, handling, and disposition, documented to provide an audit trail.
- **Cryptographic Erasure:** A data sanitization method that destroys the encryption keys used to access encrypted data, rendering the data unrecoverable while preserving the usability of the storage medium.
- **Degaussing:** The process of using a strong magnetic field to neutralize the magnetic domains on a hard drive or other magnetic storage media, thereby destroying the data.
- **IT Asset Disposition (ITAD):** The secure, compliant, and environmentally responsible process of retiring, recycling, and reusing electronic assets at the end of their useful life.
- **NIST 800-88 Revision 1:** A set of guidelines from the National Institute of Standards and Technology for media sanitization, which includes recommended methods such as "Clear," "Purge," and "Destroy".
- **Protected Health Information (PHI):** Any health information that is created or received by a covered entity and relates to the past, present, or future physical or mental health of an individual.
- **R2v3:** A globally recognized certification for electronics recyclers, focused on environmental and public health standards for the disposition of electronic equipment.

Appendix B: Sample Certificate of Destruction

This certificate provides documented proof of the destruction of data on retired IT assets. It typically includes:

- **Client Information:** Name and contact details of the client.
- **Service Provider Information:** ITUpcycle LLC's name and contact details.
- **Date of Service:** The date the service was completed.
- **Asset List:** A detailed, serialized list of all data-bearing devices destroyed, including manufacturer, model, and serial number.
- **Official Signature:** The signature of an authorized representative of ITUpcycle LLC, certifying that the destruction was performed in accordance with this policy and relevant legal standards.